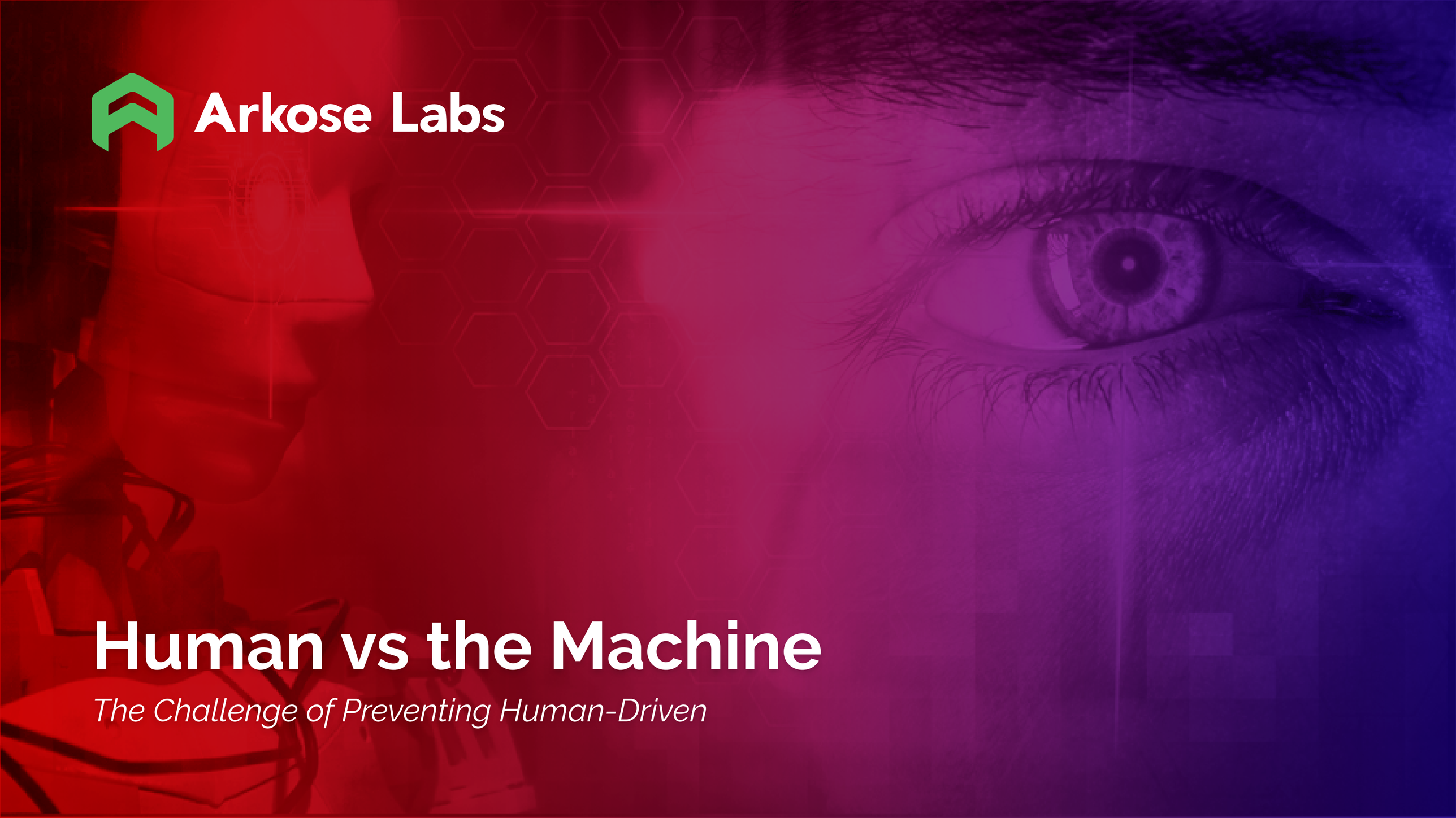


Human vs the Machine

The Challenge of Preventing Human-Driven

The Rise of Human-Driven Fraud

Fraud attack patterns are constantly evolving, and fraudsters have realized that there is huge profit to be made from playing the long game. They are investing in long-term strategies, launching multi-step attacks that disguise their fraudulent intent.

Traditionally the highest volume of fraud has been automated - ranging from basic bots to highly sophisticated bots, trained to mimic human behavior. However, there has been a recent trend towards more human-driven attacks as fraudsters invest in more sophisticated techniques. They attempt to blend in with legitimate traffic, circumventing fraud prevention technology designed primarily to detect automated attacks.

This has resulted in a significant rise in the use of human fraud farm or click farms. These are large-scale operations where fraudsters hire low-paid workers who use multiple devices to mount fraud attacks at scale. These attacks are more difficult to detect, as they use a range of tactics to appear legitimate.

To avoid potential losses, businesses need to adapt their fraud prevention efforts to incorporate defenses specifically designed to root out large-scale human-driven attacks.

Fraudsters' Strategic Approach to Maximizing Returns

With the growth of more complex fraud attacks on digital businesses, fraudsters are experimenting with the best tactics to drive the biggest return on investment. They use a hybrid of human resources and automated tools to launch sophisticated, targeted attacks that maximize financial gain.

These attack patterns have developed alongside the evolution of advanced fraud prevention strategies. Attackers reverse engineer anti-fraud technologies to ascertain the data used to differentiate fraud from good customers, and tailor their attacks accordingly to trick systems.

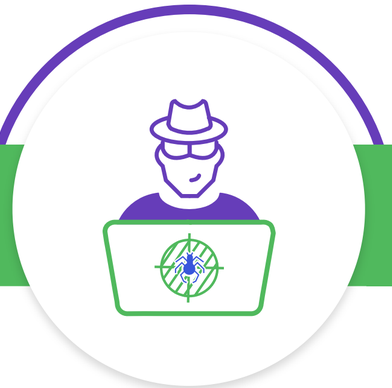
Fraudsters coordinate attacks according to the industry and customer base. In more complex attacks, automated tools will be used to lay the groundwork, for example carrying out large-scale identity credential testing, targeting the account sign-up process. As multi-step attacks progress, there will be greater reliance on more intelligent technologies and human resources.

Understanding these trends and the economic incentives behind fraudsters' methodology is vital in creating effective and long-lasting fraud defense.

The Human-Driven Fraud Continuum

Complex, hybrid fraud attacks are launched by fraudsters who combine intelligent, automated bots with a network of human fraud farm resources. The bots are designed to recognize challenges that require human interaction. Where there is high profit potential, bots redirect these challenges via applications to fraud farm networks, where workers complete the authentication process.

Lone fraudster plans attack and coordinates the required resources.



Lone fraudster deploys large-scale attacks using bots.

When automated attacks meet resistance, bot is coded to escalate to a human.

Bot connects to applications which connect fraudsters to distributed fraud farm resources.

Fraud farm workers complete authentication challenges.

Major Trend – Human vs the Machines

There was a huge spike in human-driven fraud at the end of 2019, with Arkose Labs detecting a 90% increase in this type of abuse. For example, during this time, more than half of fake account registrations on social media platforms came from humans. Additionally, the Arkose Labs network identified a series of human-driven attacks originating in China, the USA, India, Brazil and Russia, where fraudsters set up fraudulent accounts to abuse promotions offering free server time to mine for Bitcoin.

Due to the higher overheads incurred by using human labor, fraudsters will only do this where there is a significant return on investment. Human-driven fraud is particularly effective in social media, retail and online gaming platforms where actions such as completing a purchase or creating an account require human logic, making it harder to perform automatically.

The Faces of Human-Driven Fraud

Fraud prevention strategies are developing increasingly advanced ways of detecting automated attacks. This has led fraudsters relying more on human resources and developing inventive ways to monetize customer interactions. In general, attacks with a major human element are a great deal more costly than automated attacks.

Highly skilled fraudsters

Fraudsters will plan and orchestrated multi-step attacks, focusing their strategies on how best to monetize attack vectors. They will tap into support services in an evolved cybercrime ecosystem to execute multi-stage attacks.

Physical fraud farm

These are organized operations where teams of low-skilled, low-cost workers are hired to work in physical fraud farm. They work en masse to bypass measures that detect automated attacks.

Distributed network

Workers login via applications from across the globe to help with hybrid, orchestrated attacks. Their different IP addresses and fingerprints make coordinated attacks more difficult to detect. They work on demand and represent the gig economy for fraud.

Attackers Will Invest More for a High Monetization Potential

Financial incentives behind fraud vary across the globe and are influenced by a range of factors including:

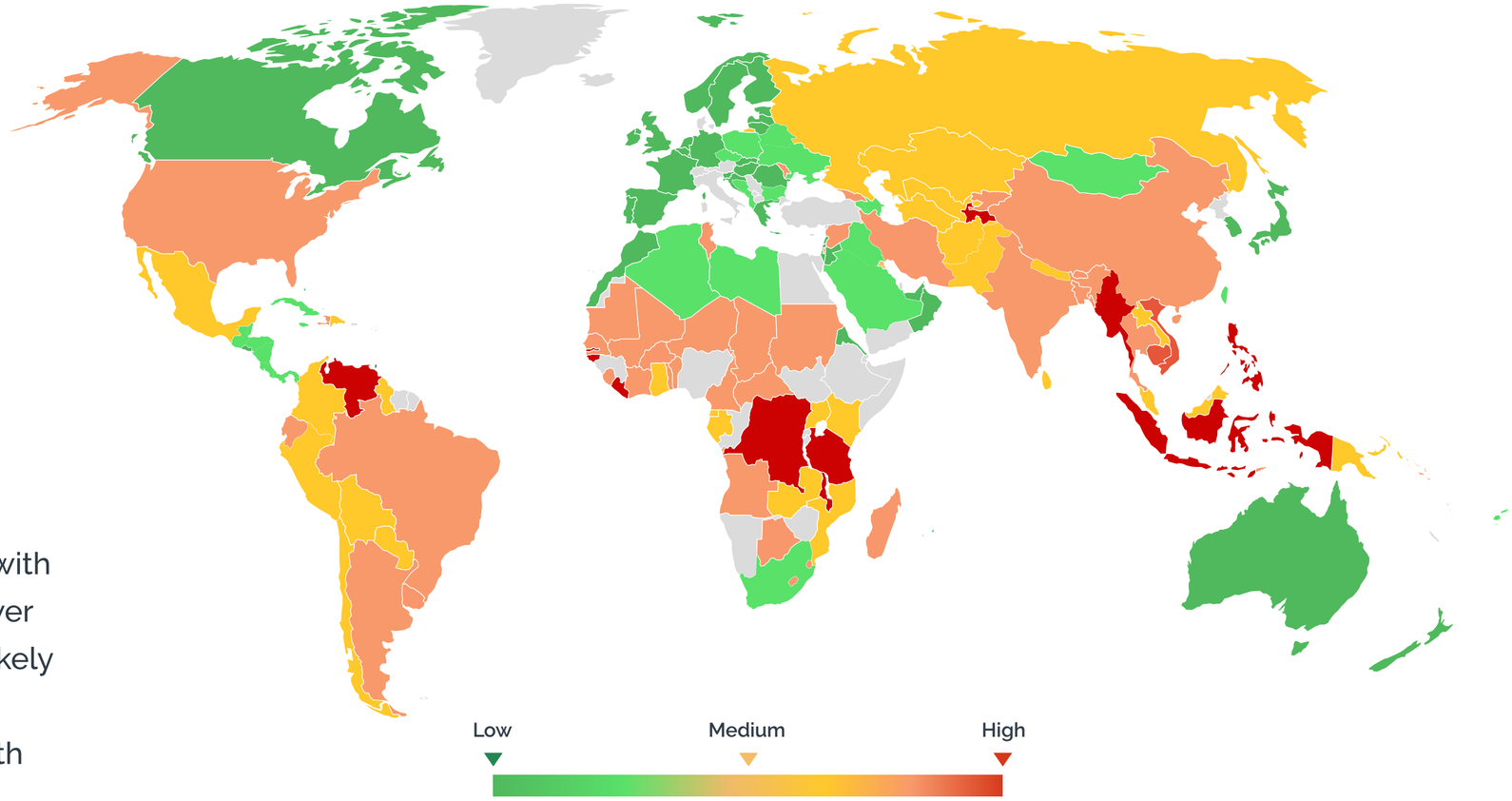
Wages

Cost of labor

Living costs

Access to technology

Value of different currencies

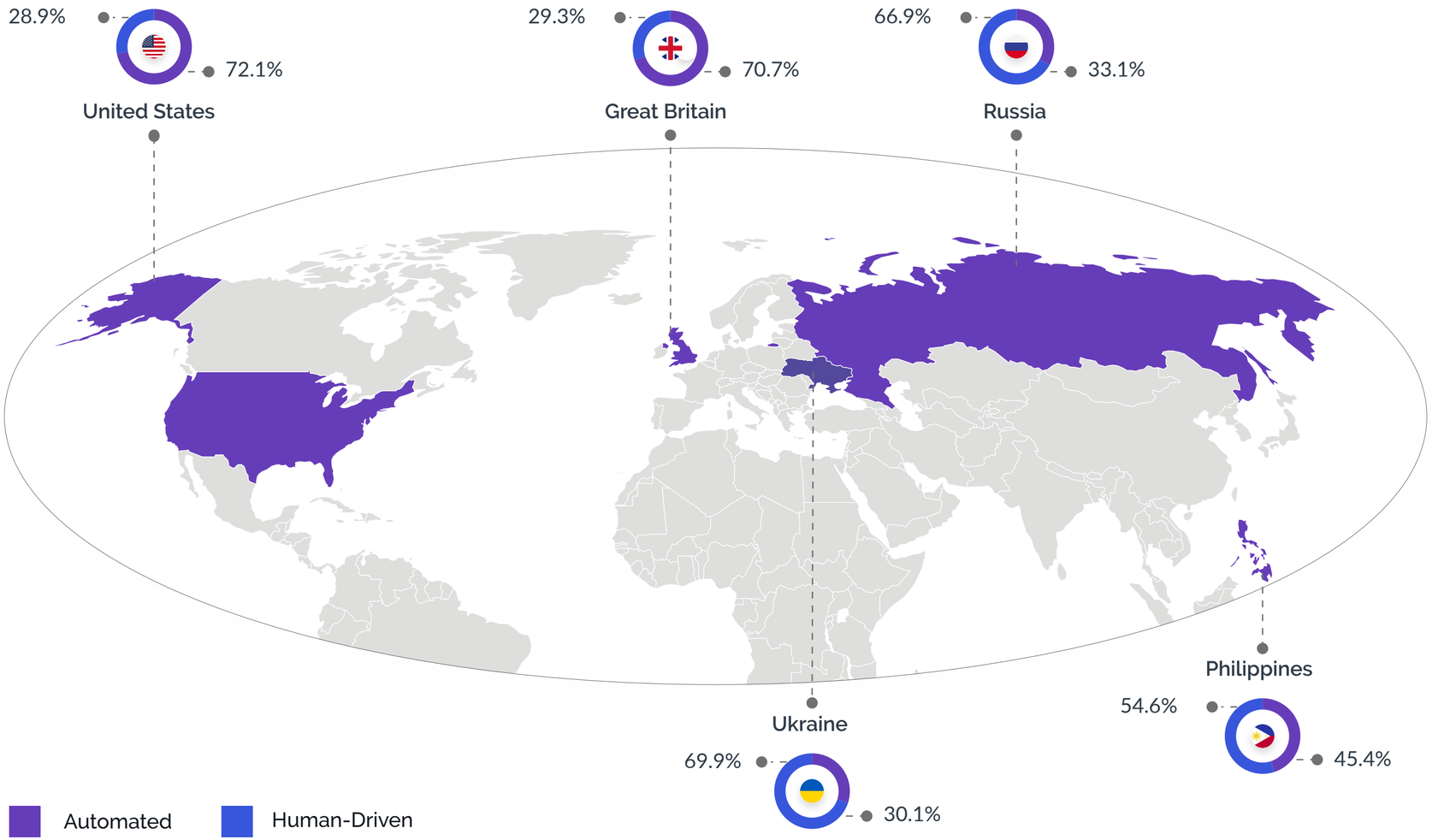


Generally fraudsters from countries with lower economic stability have much more to gain from cybercrime, especially when attacking countries with stronger currencies. The cost of labor is much lower in these countries and as a result fraudsters are likely to invest more resources into their efforts, and persevere for longer than average when faced with friction.

Fraudsters Tap into Low-Cost Human Labor Pools

While attacks from economically prosperous nations such as the USA and Great Britain still tend to be automated, there has been a notable rise in human-driven attack patterns from less economically developed countries, where labor is cheap and workers' rights are limited.

The key countries of origin for human-driven fraud shifted in the final quarter of 2019*, with fraudsters escalating their use of human fraud farm to minimize cost, and maximize return. Fraud farm-driven attacks grew considerably in Venezuela, Vietnam, Thailand and India, and attacks from the Philippines, Russia and Ukraine almost tripled compared to Q2 2019.



*Arkose Labs' Q1 2020 Fraud report

The Challenge of Identifying Human-Driven Fraud

Human-driven fraud requires a different approach to preventing automated attacks. Human click farms can easily clear challenges aimed at rooting out bots and are doing so in huge numbers. There are, however, notable differences between click farm traffic and genuine customers. Malicious users display different behavior patterns, for example often moving much faster or slower than authentic users.

Traditionally businesses have focused on fraud mitigation rather than prevention, accepting that some fraud is a 'cost of doing business'. This has allowed fraudsters to hone their techniques over time, learning from past attempts. Despite serious investment in fraud prevention strategies, fraudsters have been able to evolve at a faster rate and keep in the driving seat.

Businesses need a strategy that dynamically adapts to the threat landscape and provides robust protection against fraud. This requires an intelligent combination of risk-profiling and targeted step-up challenges, that dramatically reduces the profit margin for fraudsters.

1 Understanding Real-Time Signals

A vital component of any fraud prevention strategy is risk-based authentication that provides a detailed analysis of behavior patterns indicating fraud, and flags suspicious activity for secondary screening. However, it is imperative that anti-fraud systems do not take data purely at face value. Fraudsters have developed highly sophisticated methods to obscure their identities and manipulate data in order to bypass fraud prevention controls.

Deep device assessments
Analyze traffic using comprehensive device fingerprinting and device validation to ensure in-depth understanding of user characteristics and allow businesses to assess the validity of the device.

Deep network analysis
Assess the user's reputational integrity based on IP addresses and network fingerprints

Location assessment
Accurately identify location spoofing and analyze activity levels. Where activity levels are disproportionate to authentic traffic in a location, flag user as risky.

2 Assessing Each Interaction Based On Behavioral Patterns

Although the signs of human-driven fraud can be subtle, individual fraudsters and fraud farm display very different behavior patterns to legitimate customers. To identify these telltale signs, the key is to evaluate fraud pattern data harvested across different websites and apps, and then ensure the correct tools are in place to flag risky users in real time. Categorizing traffic by risk profile, fraud pattern, and attack profile forges a firm basis for powerful secondary screening.

Abnormality detection

Continuously monitor networks for unusual events or trends, and analyze network traffic patterns in real-time to enable identification of suspicious behavior patterns across cohorts.

Behavior biometrics

Analyze user interaction with their devices to identify behavioral anomalies and automation. Scrutinize elements such as keystroke patterns and speed, mouse use characteristics and cognitive biometrics, alongside other behavioral indicators such as previous sim card usage. measures obscuring IP address identity; and whether user behavior is in line with what is expected from the user location.

Machine learning

Detect malicious activity displaying similar characteristics across different use cases and times using machine learning. This enables rapid detection of emerging and subtle signs of fraud, helping to protect against evolving attack patterns across the network.

3 Time-Sapping Puzzles

In recent years, businesses have aimed to offer a frictionless experience for users. This has allowed fraud to flourish as fraudsters develop more sophisticated techniques with every attempt. As a result, this has had a significant impact on both company profits and individual customers. It is time to reassess the role of friction in balancing optimal user experience and online security. Where secondary screening is in a user-friendly form, it can strengthen the customer relationship.

Tailored challenges

Present high risk-traffic that shows signs of originating from a fraud farm with authentication challenges that deliberately waste their time and resources. This slashes their potential profit and causes them to abandon attacks.

Streamlined authentication

Deploy authentication challenges that are fun and easy for good users to complete and which can be integrated into the web or mobile experience, reducing the necessity of consumers to complete out of band authentication.

Continuous feedback loop

Learn from data acquired from enforcement challenges in order to refine the risk assessment that flags traffic as potential fraud farm activity. Accurate risk profiling at the initial stages ensures traffic is triaged effectively according to risk and there is a low impact on good users.

4 Graduated Authentication

Human fraud farm display different behavior patterns to genuine customers, as the workers operate multiple devices simultaneously. In these cases, increasingly complex challenges are needed to drain attack resources and profit potential. This is particularly effective in stopping fraud farm, as this activity is only profitable for the individual if they are able to speed through attacks, without being slowed down by challenges.

Increasingly complex puzzles

Present risky traffic with increasingly complex puzzles that require focus and engagement, for example counting totals on dice, which takes time but is still doable for legitimate users.

Insights from interactions with challenges

Analyze how users interact with puzzles, and whether they are displaying normal completion behavior. Additionally, limit the time permitted to complete a puzzle to protect against fraud farm workers that have a queue of challenges to solve.

Frustrate fraud farm

Frustrate fraudsters with not one, but multiple challenges, when behavioral biometrics and the timings provide further indication that it is originating from a fraud farm, in order to waste their time further.

Benefits of this Approach

Graduated challenges slow and frustrate attackers. Sap fraudsters' time and prevent them from directing their resources to other attacks.

Never block true users. Rather than completely blocking risky traffic, users are offered the opportunity to prove their legitimacy, reducing the risk of true users being punished due to a false positive.

Efficient authentication for legitimate customers. Maintain good customer relationships, with authentication processes that place customer experience as the top priority.

Better throughput than SMS and out-of-band verification due to a more seamless user experience. This is also a more cost-effective solution.

Protection against hybrid attacks. As fraudsters will deploy a mix of automation and human execution, even in the same attack, defenses need to be able to shift dynamically according to the style of attack and protect against both.

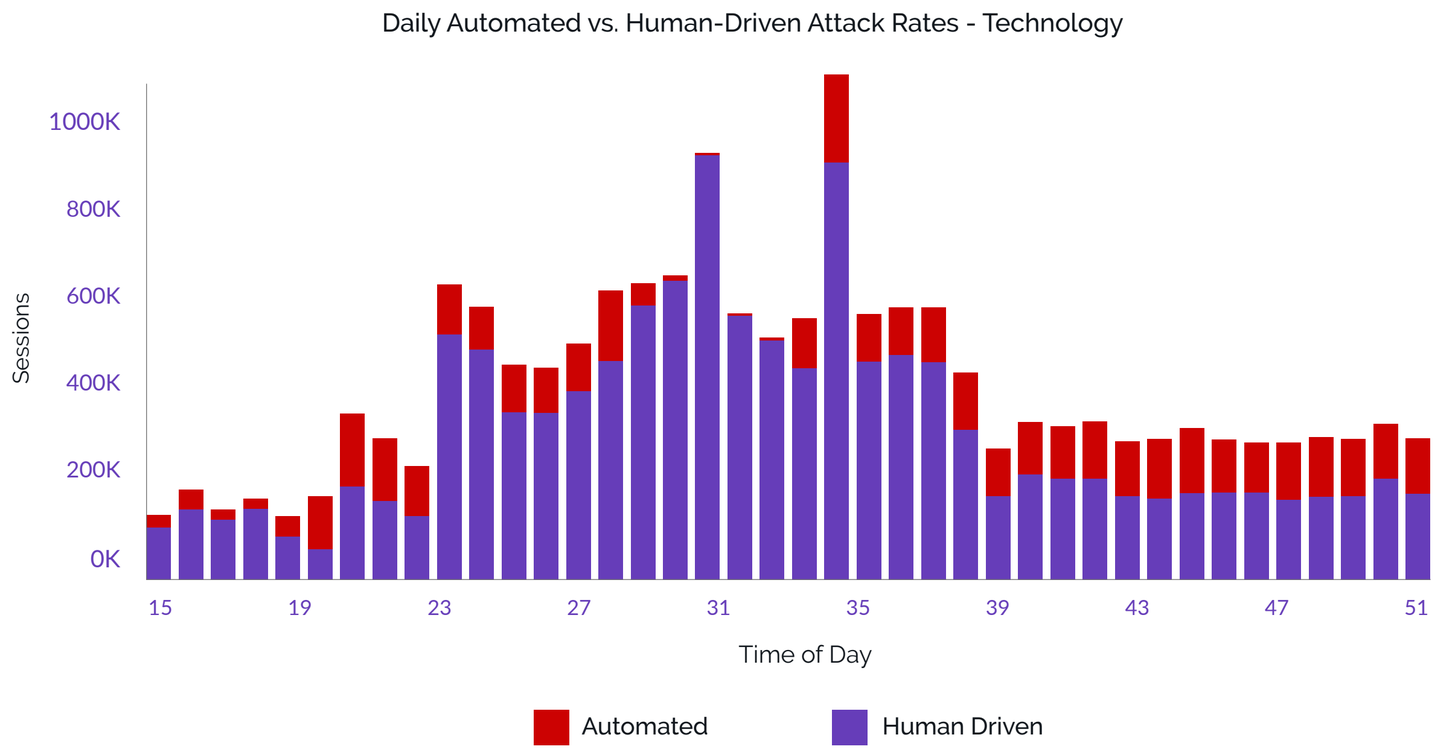
Case Study 1 Onslaught of Human Fraud Farm

Arkose Labs protects e-commerce provider from gift card fraud

Challenge:
A major fraud farm operation was launched targeting gift card transactions. Attackers were mounting tens of thousands of assaults daily, using an approach combining automation and fraud farms to maximize both volume and sophistication of attacks.

Solution:
During the defense campaign, more than 30 configuration setting measures were taken to detect attacks and add friction in order to slash the profits of the operation. Any request from the fraud ring was met with over 20 different online puzzles alongside other time-sapping measures.

Result:
The fraud farm ceased its attacks, while genuine traffic continued to flow freely.



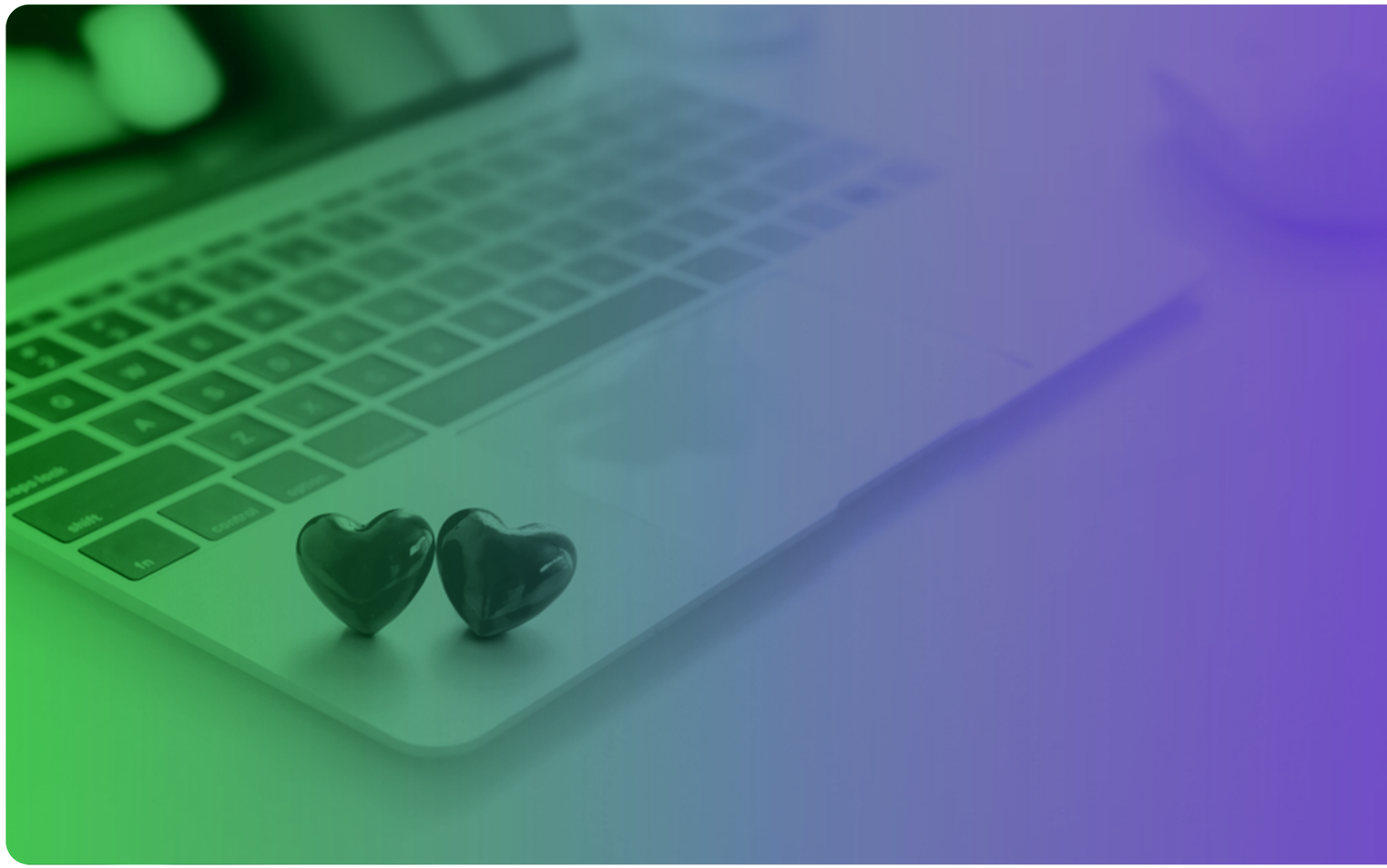
Case Study 2 Online dating platform detects targeted human-driven fraud

Romance restored by online protection from Arkose Labs

Challenge:
The online dating platform experienced an issue with “romance scams”, whereby fraudsters attempted to trick legitimate users out of money. These targeted, human attacks are notoriously difficult for traditional fraud solutions to detect and the company was struggling to detect this activity until after the abuse occurred.

Solution:
Arkose Labs deployed behavioral analytics to identify signs of fraudulent activity at the account creation stage and provide early warning of malicious activity. Fraudsters were forced to complete a range of increasingly complex authentication challenges, draining their time and resources. This drastically reduced the profit potential of the operation.

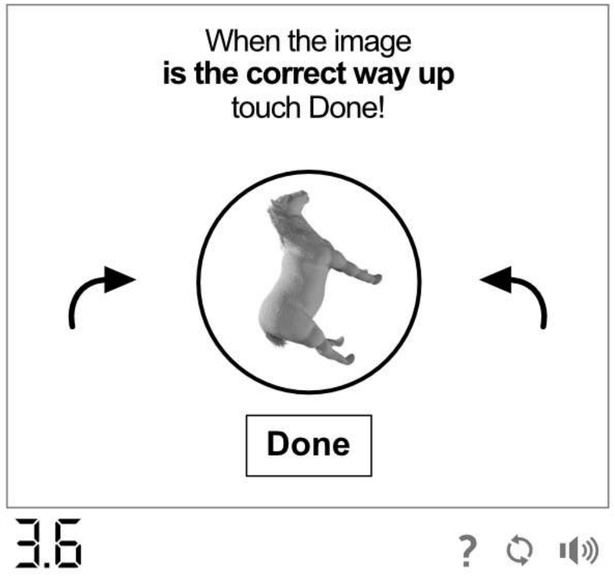
Result:
The company saw an 80% reduction in fake account registrations. Further customer abuse and spam was prevented, safeguarding the interests of genuine users.

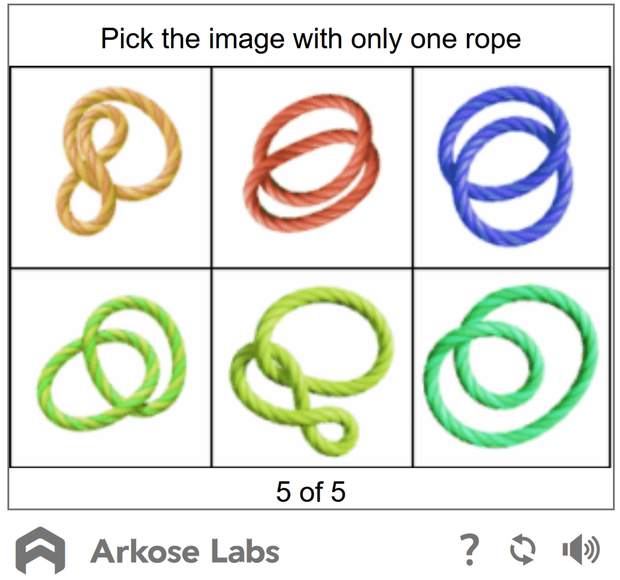


Eliminate Fraud Farm Attacks with Arkose Labs

The Arkose Labs Fraud and Abuse Defense Platform is designed to provide an optimal balance between excellent user experience, and complete protection against online fraud. This is a unique two-step platform combining Arkose Detect, a dynamic risk engine, with Arkose Enforce, which provides a range of step-up challenges tailored to the user's risk profile.

When the platform detects signs of a human fraud farm, the user is directed to a series of challenges designed to waste time and resources, making the attack expensive and unsustainable. Depending on the profile and solve pattern of the fraud farm, challenges can either be time-limited to prevent queued pipelines, or be multiplied to take a large period of time, sapping attackers efficiency. Arkose Enforce also tailors the number of challenges presented to each user based on the risk profile (within the limits pre-agreed with the customer). This is very effective in curbing the efficiency of human fraud farms and click farms.





Breaking the Business Model of Fraud

For too long, businesses have accepted fraud as a 'cost of doing business'. Fraud is a lucrative enterprise with the 2019 Official Annual Cybercrime Report predicting that by 2021, cybercrime will cause annual global losses of $6 trillion.* To ensure long-term robust protection against fraud it is essential to adopt a zero-tolerance approach to cybercrime.

Effective fraud prevention should be aimed at drastically cutting the ROI of fraud. A combination of risk-profiling and targeted authentication challenges ensure that fraudsters are forced to waste time and resources, rendering their attacks difficult and costly. Fraud prevention platforms should continue to deliver challenges beyond the attackers' capacity to complete them. This disrupts the economics of the attack making fraud financially non-viable.

Fraudsters aim for the highest possible profit margins in the shortest possible time. When they encounter sustained friction they typically pivot, focusing their attacks on other businesses. Cooperation across a broad range of companies ensures that tell-tale signs of specific attacks are shared within trusted circles. This results in gains across the entire digital commerce ecosystem, as whole fraud operations are flagged as malicious and put out of business.

Businesses need to take a robust stance against fraud to safeguard their revenue streams and maintain customer trust. This multi-step, collaborative approach ensures comprehensive fraud protection that safeguards businesses long term.

https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

About Arkose Labs

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.

Sales: (800) 604-3319
arkoselabs.com

Offices

San Francisco
250 Montgomery St 10th Floor, San Francisco, CA 94104, USA

Brisbane
315 Brunswick St, Brisbane, Queensland AU

Schedule Demo